DRAGOS

2019

YEAR IN REVIEW

LESSONS LEARNED FROM THE FRONT LINES OF ICS CYBERSECURITY

CONTENT

EXECUTIVE SUMMARY 3

2019 KEY FINDINGS 4

KEY RECOMMENDATIONS FOR IMPROVEMENT 4

INTRODUCTION 5

WHAT IS ON YOUR INDUSTRIAL NETWORK? 6

IS YOUR INDUSTRIAL NETWORK UNDER ATTACK? 8

HOW DO YOU RESPOND TO A CYBER ATTACK ON YOUR INDUSTRIAL NETWORK? 13

CONCLUSION: A CALL TO ARMS 16

APPENDIX 18

EXECUTIVE SUMMARY

IN 2019, THE DRAGOS PROFESSIONAL SERVICES TEAM OBSERVED AND RESPONDED TO AN INCREASE OF CYBER ACTIVITY TARGETING CRITICAL INDUSTRIAL INFRASTRUCTURE.

Threats focusing on these organizations continue to adapt and mature, gaining more advanced capabilities to attack industrial control systems. These adversaries largely remain unchecked by defenders, stemming from a combination of both the lack of visibility in industrial environments and our community's lack of understanding and communication around the potential impacts of a cybersecurity incident on control systems.

Understanding today's evolving cyber threat landscape - through a deep understanding of how adversaries behave and the potential operational, safety, and financial impacts they can cause - is vital for the industrial control systems (ICS) community to raise the bar in cybersecurity and secure the resources needed to effectively protect the processes civilization depends on daily.

This report - compiled from the engagements performed throughout 2019 in customer environments by our threat hunting, penetration testing, incident response, tabletop exercise, and assessments teams - provides the ICS community with first-hand insights to understand the state of ICS cybersecurity, what the impacts are for the community overall, and recommendations to improve ICS cybersecurity strategies for all organizations' maturity levels and goals.

2019 KEY FINDINGS

The Dragos Professional Services team's 2019 key findings--gathered from performing proactive and responsive assessments across various industries, focused on energy, electric, manufacturing, transportation, and water--revealed a vast knowledge gap throughout the community, impacting network visibility, detection capabilities, and incident response preparedness.

100% of organizations had routable network connections into their operational environments

71% of organizations assessed had poor security perimeters, allowing the Dragos Red Team to traverse and gain access into the ICS networks

76% of organizations could not detect Dragos' Red Team activities

66% of incident response (IR) cases involved adversaries directly accessing the ICS network from the Internet

0% of IR cases were facilitated by aggregated logging or visibility into the ICS networks. Every incident required manual retrieval of logs and distributed analysis

KEY RECOMMENDATIONS FOR IMPROVEMENT

In response to these findings, Dragos' recommended areas of focus for industrial organizations in 2020 include devoting significant resources and investments in:

- ICS network visibility and asset identification/ management (Collection Management Framework[1] and Crown Jewel Analysis)[2]
- ICS network monitoring with detection capabilities for advanced techniques, tactics, and procedures based on intelligence of threats and adversary group activity
- ICS threat detection capabilities mappable to the MITRE ATT&CK Framework for ICS[3]
- Network segmentation strategies and reinforced ICS perimeters
- ICS incident response data collection and forensics
- ICS incident response communication planning

INTRODUCTION

ICS CYBERSECURITY REQUIRES MORE THAN APPLYING CONTROLS, UNDERSTANDING THREATS, OR COMPLYING TO STANDARDS--IT MUST BE A BUSINESS CULTURE AND SUSTAINABLE PROGRAM THAT PROTECTS THE ORGANIZATION, ITS PEOPLE, AND THE COMMUNITY.

Threats to our critical infrastructure continue to increase in both frequency and sophistication, threatening the very processes we depend on in our everyday lives, such as clean, running water and reliable power generation. Adversaries are finding new ways to compromise the systems that ensure these processes run safely and efficiently, which must be met with new cybersecurity strategies to combat them--strategies rooted deep within an understanding of these adversaries and the resources it takes to combat them.

Whether organizations have mature ICS cybersecurity strategies or are just getting started down the path of better defense, there are three foundational questions each should have the knowledge to confidently answer: What is on your industrial network? Is your industrial network under attack? How will you respond to a cyber attack?

Answering these questions provide the basis for any ICS cybersecurity program--which needs to stretch across the boundaries of IT, OT, engineering, finance, management, and executive leadership. Every organization working with industrial processes needs to understand how security benefits their business, manages risk, and protects safety. In 2019, multiple clients engaged Dragos to help mature their ICS cybersecurity program--and in each case, these questions were invaluable to focus their efforts and resources.

WHAT IS ON YOUR INDUSTRIAL NETWORK?

With the convergence of IT and OT environments, the cyber threat landscape continues to expand, resulting in increased attack vectors and growing risks to ICS/ OT-specific operations.

While some industrial organizations are beginning to understand these associated impacts, many still lack the appropriate protections needed to sufficiently secure their industrial processes. In 2019, Dragos observed an overall lack of investment toward sustainable strategies to reduce the risk linked to cyber incidents on OT networks. This first foundational question, what is on your industrial network?, has three main components, that can be broken down into a maturity model approach for any organization to answer:

01 CRAWL

ESTABLISH VISIBILITY INTO THE ICS/OT NETWORK

You cannot protect what you do not know or properly assess risk management capabilities without understanding what you are trying to protect. Quantify the operational, safety, physical, and financial impact associated with a loss, disruption, or malicious attack of the industrial network.

02 WALK

ESTABLISH A COLLECTION MANAGEMENT FRAMEWORK

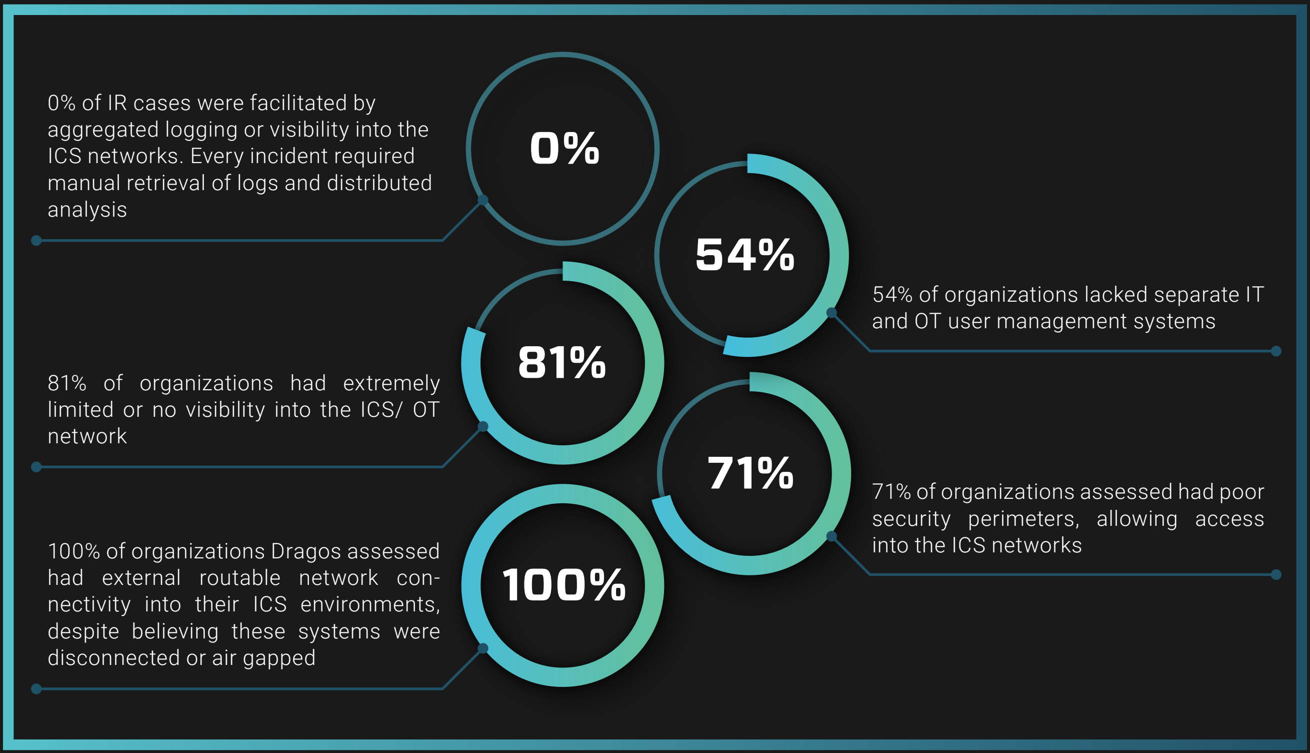
Structure your ICS/OT environment and prepare for cyber threats. Establish segmentation strategies to protect the ICS network from the corporate network and internet, leveraging firewalls and other technologies. These should include specific rules based on Step 1 (crawl) and your understanding of the network.

03 RUN

TAKE FULL ADVANTAGE OF DETECTION TECHNOLOGIES LEVERAGING THREAT INTELLIGENCE SPECIFIC TO ICS/OT NETWORKS

Have trained personnel across IT security, OT security, engineering, and management that can act on threat intelligence associated with OT-specific issues.

DRAGOS WORKED WITH SEVERAL ORGANIZATIONS IN 2019 THAT LACKED CAPABILITIES TO IDENTIFY WHAT WAS ON THEIR NETWORKS, IMPACTING THEIR ABILITY TO DETECT AND RESPOND TO MALICIOUS ACTIVITY FROM EITHER ASSESSMENTS OR ADVERSARIAL ACTIVITY.



0% of IR cases were facilitated by aggregated logging or visibility into the ICS networks. Every incident required manual retrieval of logs and distributed analysis

54% of organizations lacked separate IT and OT user management systems

81% of organizations had extremely limited or no visibility into the ICS/ OT network

71% of organizations assessed had poor security perimeters, allowing access into the ICS networks

100% of organizations Dragos assessed had external routable network connectivity into their ICS environments, despite believing these systems were disconnected or air gapped

THE BASICS FOR ANY ICS/OT-SPECIFIC CYBERSECURITY PROGRAM NEEDS TO ADDRESS RISK MANAGEMENT FOR THE INDUSTRIAL ORGANIZATION.

This will ensure that the asset owner and operator invest in sound technologies, repeatable processes, and trained personnel associated with the risk. Unfortunately, the impacts associated with ICS/OT-specific cybersecurity incidents can far outweigh any financial impacts associated with traditional IT systems. ICS/OT networks, if compromised, can involve expensive equipment breakdown, property damage, and injury or even loss of life. An organization needs to understand these impacts first and foremost, then trace those impacts back to the critical processes and systems that need to be protected. We call this “crown jewel analysis” and associate it with an architecture review and “crawling stage” for this first foundational question.

Once organizations understand the impacts, we recommend investing in the “people, processes, and technologies” that support securing critical systems from those impacts. This would include network segmentation, identity and access management, and basic “cyber hygiene” in the ICS environment.

Lastly, a one-two punch of ICS/OT-specific detection and threat intelligence, for mature organizations ready to “run,” will ensure you are informed and ready when it comes to cyber risk in your ICS environment. Bad guys beware; you know they are coming, and you know what to do.

IS YOUR INDUSTRIAL NETWORK

UNDER ATTACK?

It is imperative industrial organizations understand how cyberattackers leverage knowledge of industrial processes, control systems, and vulnerabilities in order to detect and prevent cyberattacks from being successful and causing catastrophic impacts.

If an organization has not invested in security perimeters, both digital and physical, then one suggested technique to ensure critical systems are safe and protected is to perform a threat hunt.[4] This presumes that your systems are already compromised and "hunts" for adversaries.

Similar to the first question, this can be broken down into a simple maturity model for any organization to start to tackle, regardless of their size, budget, or industry:

01 CRAWL

ESTABLISH AN ICS/OT-SPECIFIC THREAT AND VULNERABILITY MANAGEMENT PROGRAM

This does not need to be formal, at first, and can involve ingesting ICS threat intelligence and vulnerability data relevant to the industrial environment. This program should include consideration for potential impact to the specific process(es) using a consequence-driven approach. While vulnerability management is important and should be a stepping stone to maturing the network security posture, it should be prioritized with first understanding the specific weaknesses introduced by the vulnerabilities and the consequence. Combine this with MITRE ATT&CK Framework for ICS you'll gain an understanding of how adversarial use of legitimate functionality and behaviors should then become the primary focus.

02 WALK

CONDUCT MANAGED THREAT HUNTS AND PENETRATION TESTS

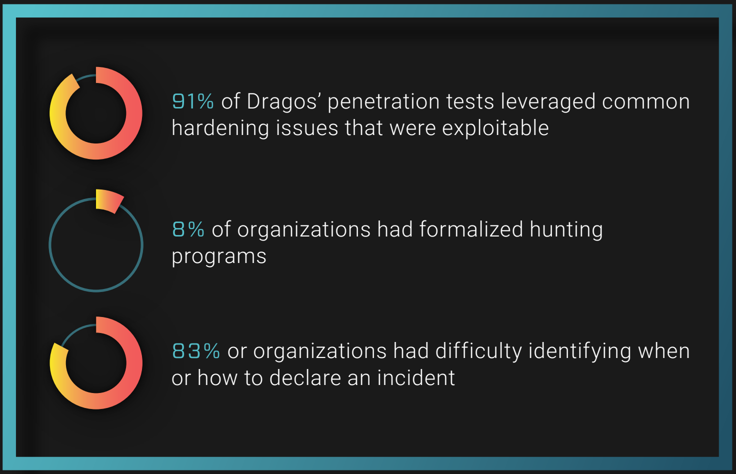
Combined with a strategy to collect relevant data in order, threat hunts and penetration tests can be conducted in a safe manner without impact to operations. This requires a trained team or external resources that are able to work with threat and vulnerability management techniques specific to ICS environments.

03 RUN

ACHIEVE ICS-SECURITY NIRVANA

Tie the threat and vulnerability programs to an overall risk management program for ICS security that informs the organization of associated cyber risks, industry trends, and organizational needs. When combined with active threat hunting, this screams "we know the risk, we know the threats, and we're making sure we are covered in the event of bad guys coming in."

UNFORTUNATELY, OUR ENGAGEMENTS IN 2019 HIGHLIGHTED THAT MANY ORGANIZATIONS WERE NOT QUITE CRAWLING, LET ALONE WALKING.

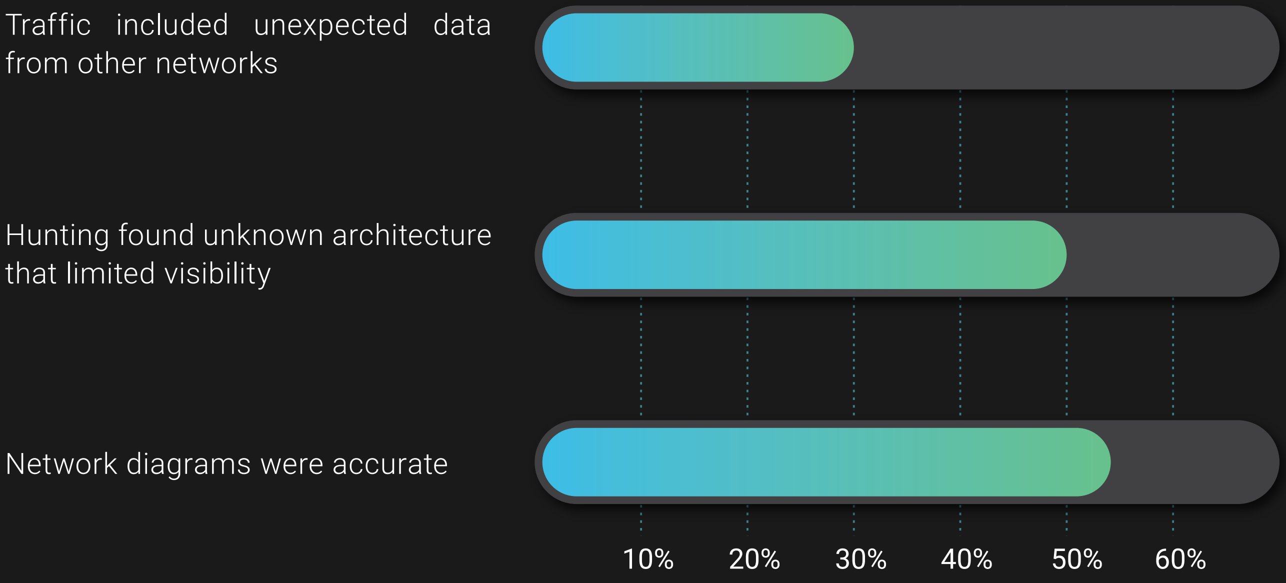


91% of Dragos' penetration tests leveraged common hardening issues that were exploitable

8% of organizations had formalized hunting programs

83% or organizations had difficulty identifying when or how to declare an incident

While it is true that many industrial devices have well-known and exploitable vulnerabilities, there are equally well-known strategies to thwart bad guys from doing harm. However, before an organization can even get there it is imperative to know exactly what is happening in your systems and creating an action plan around findings from both threat hunting and penetration testing activities. Leverage a red team--don't let the bad guys be the first time you discover something in your ICS environment.



As observed by the Dragos Threat Intelligence team and reported in the 2019 Year in Review Report, The ICS Threat Landscape, threat activity groups - such as the latest publicly-disclosed group, WASSONITE - rely on capturing valid credentials to move laterally in the enterprise network to eventually pivot into ICS/OT networks, confirming an unfortunate but common trend within industrial cyber activity:

ADVERSARIES ARE BECOMING INCREASINGLY SOPHISTICATED AND ADOPTING BEHAVIORS SPECIFIC TO ICS ENVIRONMENTS.

76% of organizations could not detect Dragos' pivoting and privilege escalation

100% of organizations had routable network connections into their environments, despite believing their ICS systems were disconnected or air-gapped, with no visibility or threat detection into the communications

71% of organizations had poor security perimeters, allowing access to their ICS network

66% of the incident response cases involved adversaries directly accessing the ICS network from the Internet

THE MOST COMMON METHOD OF LATERAL MOVEMENT AND PRIVILEGE ESCALATION REVEALED BY DRAGOS PENETRATION TESTING CONTINUES TO BE VALID CREDENTIAL RECOVERY.

91% of ICS penetration tests exploited common hardening issues

54% of organizations did not separate corporate user management from the ICS environment

86% of organizations contained ineffective logging configuration

61% of organizations lacked logging

The belief that an environment is air-gapped leads to a lack of basic cybersecurity hygiene within that network. Poorly managed firewall rules allow adversaries to traverse between trust zones, potentially allowing them to access critical ICS networks. A DMZ adds an extra hurdle for the attacker and creates a choke point for traffic, which also makes threats easier to identify. Endpoint hardening also significantly increases the difficulty for adversaries to escalate privileges and move laterally. Hardened systems can force adversaries to take a much noisier approach and increase their chances of detection (so long as network monitoring and logging are in place).

Leveraging routine threat hunting and red team assessments built from the latest threat intelligence and in-field experience demonstrates advanced defense tactics, techniques, and procedures (TTPs) like those referenced above and helps organizations proactively defend against threats to critical infrastructure before they become a potential target.

THE MORE WE KNOW ABOUT THE THREAT LANDSCAPE AND ADVERSARY BEHAVIORS, THE MORE WE ENABLE A BETTER UNDERSTANDING OF HOW ADVERSARIES CAN INTERACT WITH OUR INDUSTRIAL ENVIRONMENTS.

HOW DO YOU RESPOND TO A CYBER ATTACK ON YOUR INDUSTRIAL NETWORK?

INCIDENT RESPONSE PLANS

MANY ORGANIZATIONS ARE OVERWHELMED WITH THE IDEA OF A CYBER INCIDENT RESPONSE PLAN.

Even if you know your systems inside-out and have a sustainable threat and vulnerability management program, maintaining a team for incident response may be difficult. It does not have to be, and incident response--like all other aspects of these questions--can be tailored to your organization. It is critical for operations, safety, and business interruption concerns that asset owners and operators know what to do when a bad day happens.

01 CRAWL

UNDERSTAND WHAT A CYBERSECURITY INCIDENT LOOKS LIKE AND WHERE ONE MAY OCCUR IN TERMS OF OPERATIONS

When "crawling," your entire incident response plan may involve knowing who to call and how to preserve evidence for an external incident response team.

02 WALK

MANAGE AN ACTIVE ICS INCIDENT RESPONSE TEAM, WITH TRAINING, AND INCLUDE TABLETOP EXERCISES.

Exercises will ensure the team "trains like it's game day," and can be active participants in other steady-state ICS security programs like threat and vulnerability management.

03 RUN

TIE INCIDENT RESPONSE LESSONS LEARNED TO ICS CYBERSECURITY IMPROVEMENTS AND REDUCTION IN OVERALL CYBER RISK FOR THE ORGANIZATION.

Incident Response lessons should drive change. It should drive improvements on visibility into ICS/OT environments and how they operate, prioritizing what assets and systems need defended, and mapping your response plans and strategies to those.

IN 2019, DRAGOS OBSERVED THAT ORGANIZATIONS NEED TO INVEST IN ROBUST INCIDENT RESPONSE HANDLING, TYING THESE ACTIVITIES TO THE KNOWLEDGE OF IMPACTS, THREATS, AND VULNERABILITIES FACING INDIVIDUAL ORGANIZATIONS.

For example:

67% of Table Top Exercises required additional preparation as a key finding. In multiple instances, the incident response plan (IRP) was not known or referenced by the analysts responsible for performing the response.

Triaging and analyzing event artifacts are generally the first steps to recognizing whether an incident has occurred. The threshold for declaring an incident has occurred or is occurring depends on factors such as recognizing threat behaviors and tactics, mission requirements, and laws and regulations.

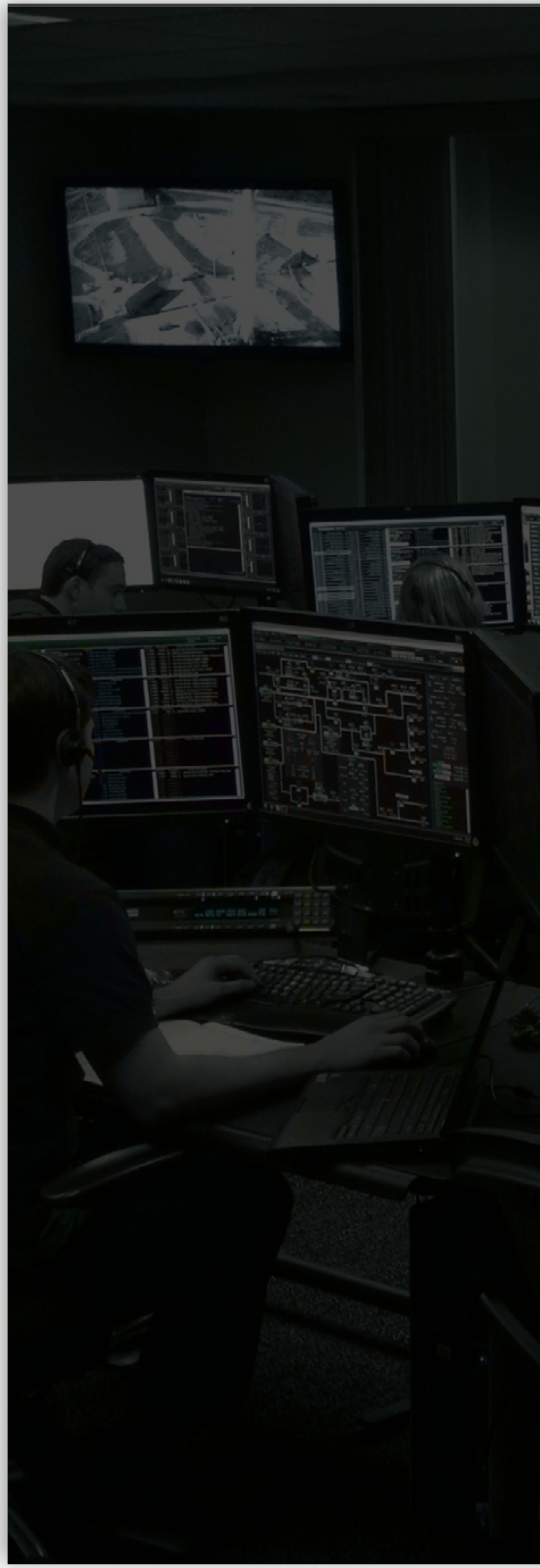
A large majority of organizations' incident declaration thresholds, defined within their IRPs, were not up-to-date with current mission requirements or the latest adversary behaviors and tactics.

RESPONSE, REMEDIATION, AND RECOVERY TO AN INCIDENT ON INDUSTRIAL NETWORKS REQUIRES A SPECIAL SKILLSET, DUE TO THE POTENTIAL IMPACT OF - AND TO - THE SYSTEM.

If an incident is found, organizations' architecture and visibility determine the level of effort to respond. In every IR case handled by Dragos in 2019, forensic artifacts had to be manually retrieved, drastically increasing the time required to triage and respond to an incident.

90% of incidents involved shared credentials for lateral movement - either through local system or vendor default accounts

0% of IR cases were facilitated by aggregated logging or passive visibility into the ICS networks. Every case involved manual retrieval of logs and distributed analysis



ORGANIZATIONS MUST CREATE INCIDENT DECLARATION THRESHOLDS OR ADJUST THEIR CURRENT INCIDENT RESPONSE PLAN TO MEET THE CURRENT THREAT LANDSCAPE. THIS WILL IMPROVE THE OVERALL RESPONSE AND INCREASE THE SPEED OF INCIDENT DETECTION,

especially when combined with information from the first two questions. Plans and investigation playbooks should include context for alerts and notifications, as well as provide step-by-step guidance to triage critical alerts. It is imperative these plans be updated regularly to ensure security teams are versed in incident response best practices and have access to the most useful and relevant information.

Add a communication plan or annex to incident response plans. Communications plans should govern all communications within the activated response team and with external stakeholders, including media. The plan needs flexibility; an organization’s management may only need a portion of the incident command structure, depending on the scope and severity of the incident. Irrespective of incident intensity, organizations’ incident response teams must be in a communications mode that is appropriate to the situation. Furthermore, incident response teams must maintain this level of communication for the duration of the incident, as well as after, to ensure transparency throughout the process.

Lastly, in order to fully understand what occurred during an incident, it is critical to understand how to collect data from ICS environments while not compromising safety or operations. IT-based incident response plans will not understand the nuance of ICS technology, nor the engineering involved. These incident response plans and playbooks, inclusive of communications and data collection, must be specific to OT concerns.

CONCLUSION

A CALL TO ARMS

AS OBSERVED THROUGHOUT 2019 BY BOTH THE DRAGOS THREAT INTELLIGENCE AND PROFESSIONAL SERVICES TEAM, ADVERSARIES ARE EXPANDING THEIR FOCUS TO ADDITIONAL CRITICAL INFRASTRUCTURE AND INDUSTRIAL ENVIRONMENTS.

Threats to ICS will continue to proliferate the more adversaries invest money, time, and talent into disrupting our critical infrastructure and the processes modern civilization depends on every day.

It is imperative that we, the ICS community, continue to improve visibility into activities and threats impacting critical infrastructure; it is a shared responsibility across multiple groups-- engineering, operations, security, and vendors--and requires unique security strategies and dedicated resources. To further complicate this shared responsibility, any impact to operations due to a cybersecurity incident could have a dramatic impact including property damage and human health and safety concerns. Compounded with the inability to use traditional IT-centric tools, our 2019 report is designed to help asset owners focus on the basics, in relation to the current threat environment.

A great place to start is simplifying understanding the potential impact of a cybersecurity incident within operational environments. What does a really bad day look like? What processes are at risk? How do the communications and technology and physics work (or don't) during outages? By understanding the impacts related to a lack of security, organizations can plan and invest according to the associated risks.

Throughout this Year in Review, we highlighted cautionary tales from client engagements to help any organization mature. These "lessons learned" are designed to start a dialogue with asset owners, vendors, and communities. As we continue to examine industrial threats and activity groups, it's important to have context around the "state of ICS security" across different sectors. What are the ways we can improve? Are we responding to the threats appropriately? Or do we still have more to do?

Dragos is proud to work with the ICS security community to continue to improve industrial cybersecurity--most recently, our collaboration with MITRE to create the new ATT&CK for ICS framework, designed to help analysts, defenders, and other security practitioners better understand threat behaviors affecting industrial environments and develop defensive strategies. We will continue to keep knowledge transfer at the forefront of our products and services, so our customers and the community are armed with the most up-to-date information and tools at their disposal.

POSITIVELY, 92% OF DRAGOS' ENGAGEMENTS INVOLVED SOME TYPE OF KNOWLEDGE TRANSFER, SHADOWING, OR OTHER PERSONNEL DEVELOPMENT. ORGANIZATIONS RECOGNIZE THAT PEOPLE ARE A CRITICAL PART OF THE SOLUTION AND UNDERSTAND THAT DECREASING THE KNOWLEDGE GAP IS CRITICAL.

Along those lines, to improve our collective security posture in 2020 - to continue to Safeguard Civilization - we recommend organizations focus on establishing or improving these key components - applicable to wherever your organization is on its ICS cybersecurity journey. These technical topics can be approached by any organization to "start running" and gaining operational maturity.

Some simple steps include:

ICS NETWORK VISIBILITY

- Gain awareness about your ICS/OT network, assets, and flow of information. Without visibility, detections, triage, and response are not possible at scale

COLLECTION MANAGEMENT FRAMEWORK

- Establish a CMF to identify information about ICS/OT assets, prepare for threats, and facilitate effective investigations

LOGGING

- Centrally manage and configure event logs to collect security-related information
- Identify ICS switches and routers and configure SPAN ports for network data collection

MONITORING

- Ensure logs are viewable from a centrally-managed location
- Implement an ICS cybersecurity technology, like the Dragos Platform, to analyze network traffic and Windows Event Logs to identify ICS equipment and its role in the environment

INCIDENT DETECTION

- Implement an ICS cybersecurity technology, like the Dragos Platform, to monitor Windows Event Logs, network traffic data, ICS-specific protocols, and tradecraft

FIREWALLS

- Review ICS protocols and determine if they are required for efficient, safe, and reliable operations
- Justify protocols with reasonable business cases

NETWORK SEGMENTATION

- Segment networks with investments in security controls to separate mission-critical ICS environments from IT systems
- Validate that communications between the IT/ICS systems is necessary for operations
- Establish a security program that will manage and adapt security controls to the changing threat landscape and business needs

IDENTITY MANAGEMENT

- Implement and maintain effective Active Directories
- Store credentials in secure credential vaults or deploy an Access Management solution to significantly reduce the exposure of high privileged accounts within corporate and ICS networks
- Require Multi-factor Authentication (MFA) for access to ICS networks to increase efforts required for adversaries to pivot into the ICS
- Utilize Microsoft's Local Administrator Password Solution (LAPS) tool to configure and manage local administrator accounts within AD environments securely

SYSTEM HARDENING

- Consult your industrial control system vendor for a list of approved endpoint hardening procedures.
- Validate hardening recommendations with your ICS vendor to avoid negative impacts on the operational network

By mapping these efforts to operational risk and investing appropriately, industrial defenders can greatly improve their abilities to detect and respond to adversaries targeting control system environments.

SECURING ICS IS NOT AN END-STATE.
IT IS A JOURNEY OF CONTINUAL IMPROVEMENT.

The adversaries are constantly improving their tactics, techniques, and procedures--and as a response, Dragos will continue to adapt our technology, intelligence, and services to arm the entire community with the tools to understand them, combat them, and counter their attempts to disrupt civilization.

APPENDIX

[1] Read the whitepaper here:
https://dragos.com/CMF_For_ICS.pdf

[2] Read the whitepaper here:
https://dragos.com/wp-content/uploads/ConsequenceDrivenICSCybersecurityScoping_Dragos-1.pdf

[3] Dragos collaborated with MITRE on creating the new ATT&CK for ICS framework, designed to help analysts, defenders, and other security practitioners better understand threat behaviors affecting industrial environments and develop defensive strategies. Read more here:
https://dragos.com/blog/industry-news/a-closer-look-at-mitre-attck-for-ics/

[4] Dragos has many resources for effective threat hunting in ICS environments:
https://dragos.com/wp-content/uploads/sans-reading-room-1.pdf
https://dragos.com/resource/six-steps-to-effective-ics-threat-hunting/
https://dragos.com/blog/industry-news/threat-hunting-part-1-improving-through-hunting/
https://dragos.com/blog/industry-news/threat-hunting-part-2-hunting-on-ics-networks/